

FICHE GUIDE

CONFIGURER WIREGUARD SUR pfSENSE 2.8.1

1 – INSTALLATION DU PACKAGE WIREGUARD SUR PFSENSE

- Depuis l'interface de gestion de pfSENSE 2.8.1, ajoutez le package « Wireguard » :
 - Cliquez « System » – « Package Manager » – « Available Packages »
 - Recherchez « WireGuard » et cliquez le bouton vert « + Install » :

WireGuard	0.2.9_5	WireGuard(R) is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPSec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN. WireGuard is designed as a general purpose VPN for running on embedded interfaces and super computers alike, fit for many different circumstances. Initially released for the Linux kernel, it is now cross-platform and widely deployable. It is currently under heavy development, but already it might be regarded as the most secure, easiest to use, and simplest VPN solution in the industry.	+ Install
-----------	---------	---	---------------------------

- Cliquez le bouton vert « Confirm » et patientez pendant l'installation du package :

Confirmation Required to install package pfSense-pkg-WireGuard.

 Confirm

2 – ACTIVATION DU SERVICE WIREGUARD SUR PFSENSE

- Depuis l'interface de gestion de pfSENSE, cliquez « VPN » - « WireGuard » - « Settings »
- Cliquez la case « Enable WireGuard » :

General Settings

Enable ☒ Enable WireGuard

Note: WireGuard cannot be disabled when one or more tunnels is assigned to a pfSense interface.

- Cliquez le bouton bleu « Save » en bas de la fenêtre
- Cliquez le bouton vert « Apply Changes » pour activer le service

3 – CREATION DU TUNNEL WIREGUARD SUR PFSense

- Cliquez « VPN » - « WireGuard » - « Tunnels »
- Cliquez le bouton vert « Add Tunnel »
- Complétez la rubrique « Tunnel Configuration » et générez la paire de clés en cliquant le bouton bleu « Generate » :

Tunnel Configuration (tun_wg0)

Enable ☒ Enable Tunnel
Note: Tunnel must be enabled in order to be assigned to a pfSense interface.

Description
Description for administrative reference (not parsed).

Listen Port
Port used by this tunnel to communicate with peers.

Interface Keys

Private key for this tunnel. (Required)

Public key for this tunnel. (Copy)

[Generate](#)
New Keys

- Complétez la rubrique « Interface Configuration » en indiquant une adresse de tunnel :

Interface Configuration (tun_wg0)

Assignment [Interface Assignments](#)

Firewall Rules [WireGuard Interface Group](#)

Hint These interface addresses are only applicable for unassigned WireGuard tunnel interfaces.

Interface Addresses /
IPv4 or IPv6 address assigned to the tunnel interface. Description for administrative reference (not parsed).

Add Address [+ Add Address](#)

- Cliquez le bouton bleu « Save Tunnel » :

Peer Configuration

Description	Public key	Tunnel	Allowed IPs	Endpoint : Port	Actions
New tunnels must be saved before adding or assigning peers.					
					+ Add Peer Save Tunnel

- Cliquez le bouton vert « Apply Changes » :

VPN / WireGuard / Tunnels

The WireGuard configuration has been changed.
The changes must be applied for them to take effect.
Notice: This action may momentarily suspend active WireGuard peer connections on any changed tunnels. [Apply Changes](#)

Tunnels Peers Settings Status

WireGuard Tunnels

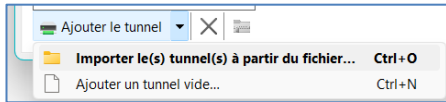
Name	Description	Public Key	Address / Assignment	Listen Port	Peers	Actions
> tun_wg0	VPN WIREGUARD	eWwxNaDDQiOznH6sSBMIINnPN2wqAsDj...	10.9.0.1/24	51820	0	+ - ↕ 🗑
+ Add Tunnel						

pfSense a maintenant une interface WireGuard logique (wg0) écoutant en **UDP/51820**.

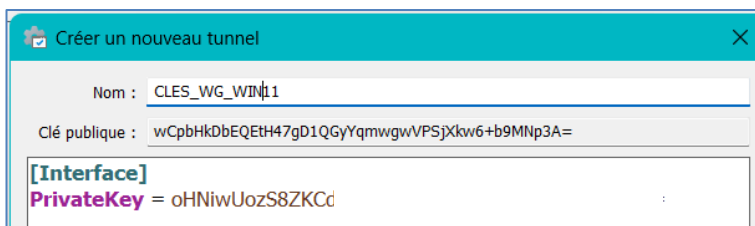
4 – CREATION D'UN « peer » (CLIENT NOMADE) SUR LE POSTE CLIENT WINDOWS

Il faut créer, ici, un « pair » WireGuard correspondant au poste Windows qui se connectera au tunnel en générant une configuration client (clé privée, publique, adresse IP, DNS, etc.).

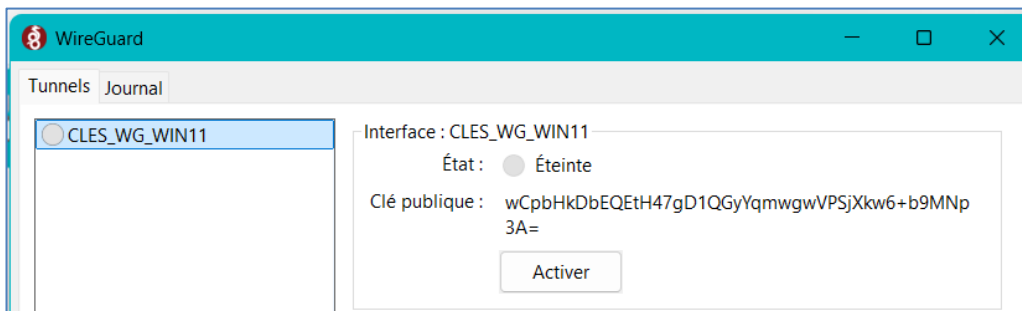
- Depuis le site officiel, téléchargez et installez le client WireGuard : [Installation - WireGuard](#)
- Double-cliquez le fichier exécutable téléchargé pour lancer l'installation ; une fenêtre s'ouvre à la fin
- Cliquez sur « Ajouter un tunnel vide... » :



- Une fenêtre s'affiche et indique une clé publique et une clé privée ; saisissez, dans la rubrique « Nom », une description et cliquez le bouton « Enregistrer » :



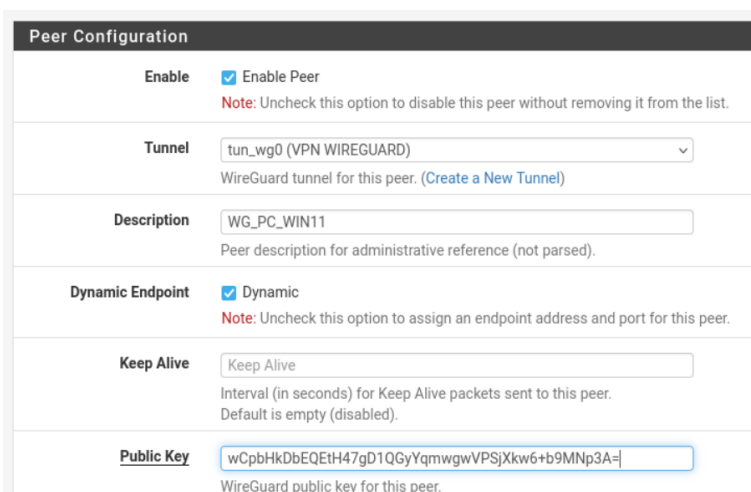
La fenêtre affiche maintenant ceci :



La clé publique devra être copiée et donnée à pfSENSE ; pour cela, copiez la clé publique.

5 – CREATION DU « peer » COTE PFSense

- Depuis l'interface de gestion de pfSENSE, cliquez « VPN » - « WireGuard » - « Peers »
- Cliquez le bouton vert « Add Peer » ; complétez la fenêtre et collez votre clé publique Windows



- Complétez la partie « Address Configuration » en indiquant une adresse IP pour le client nomade (dans le même réseau que votre tunnel – voir partie précédente) :

Address Configuration

Hint Allowed IP entries here will be transformed into proper subnet start boundaries prior to validating and saving. These entries must be unique between multiple peers on the same tunnel. Otherwise, traffic to the conflicting networks will only be routed to the last peer in the list.

Allowed IPs	10.9.0.2 / 24	Description
	IPv4 or IPv6 subnet or host reachable via this peer.	Description for administrative reference (not parsed).

Add Allowed IP + Add Allowed IP

Save Peer

- Cliquez le bouton bleu « Save Peer »
- Cliquez le bouton vert « Apply Changes » :

VPN / WireGuard / Peers

The WireGuard configuration has been changed.
The changes must be applied for them to take effect.
Notice: This action may momentarily suspend active WireGuard peer connections on any changed tunnels.

Apply Changes

Tunnels **Peers** Settings Status

WireGuard Peers

Description	Public key	Tunnel	Allowed IPs	Endpoint : Port	Actions
WG_PC_WIN11	wCpbHkDbEQEtH47g...	tun_wg0	10.9.0.0/24	Dynamic	

+ Add Peer

pfSENSE sait maintenant reconnaître le client Windows 11 grâce à sa clé publique.

6 – COMPLETER LA CONFIGURATION DU TUNNEL COTE CLIENT

- Depuis le client Windows, ouvrez la fenêtre de configuration de WireGuard
- Cliquez le bouton « Modifier » en bas à droite de la fenêtre
- Complétez la fenêtre et cliquez le bouton « Enregistrer » :

Modifier le tunnel

Nom : CLES_WG_WIN11
Clé publique : wCpbHkDbEQEtH47gD1QGyYqmwgwVPSjX

Clé publique de votre machine Windows

Clé privée de votre machine Windows

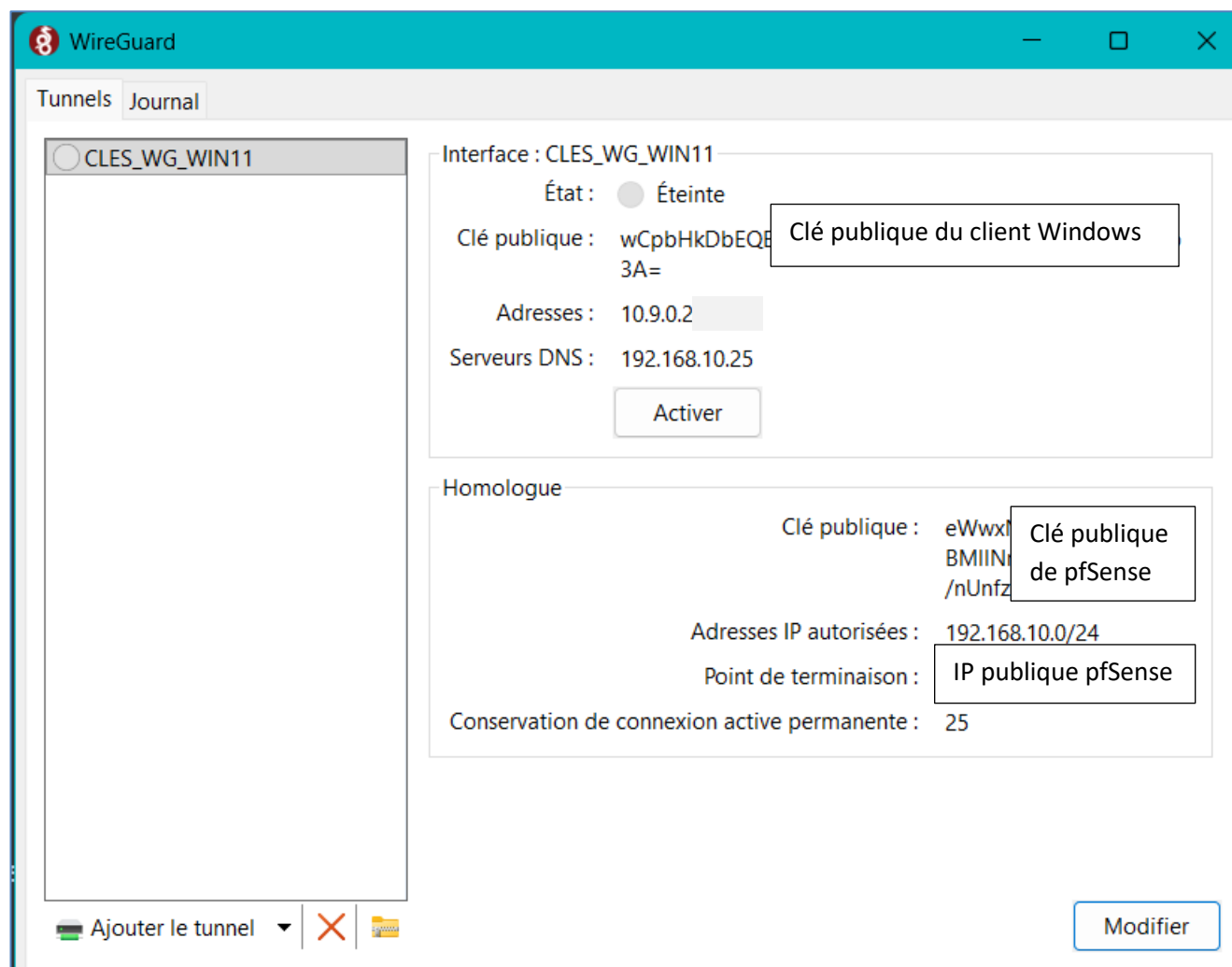
[Interface]
PrivateKey = oHNjwI In7SRZH
Address = 10.9.0.2 /24
DNS = 192.168.10.25

[Peer]
PublicKey = <clé publique du pfSense>
Endpoint = <ton IP publique>:51820
AllowedIPs = 192.168.10.0/24
PersistentKeepalive = 25

Collez, ici, la clé publique de pfSense et saisissez votre adresse IP publique

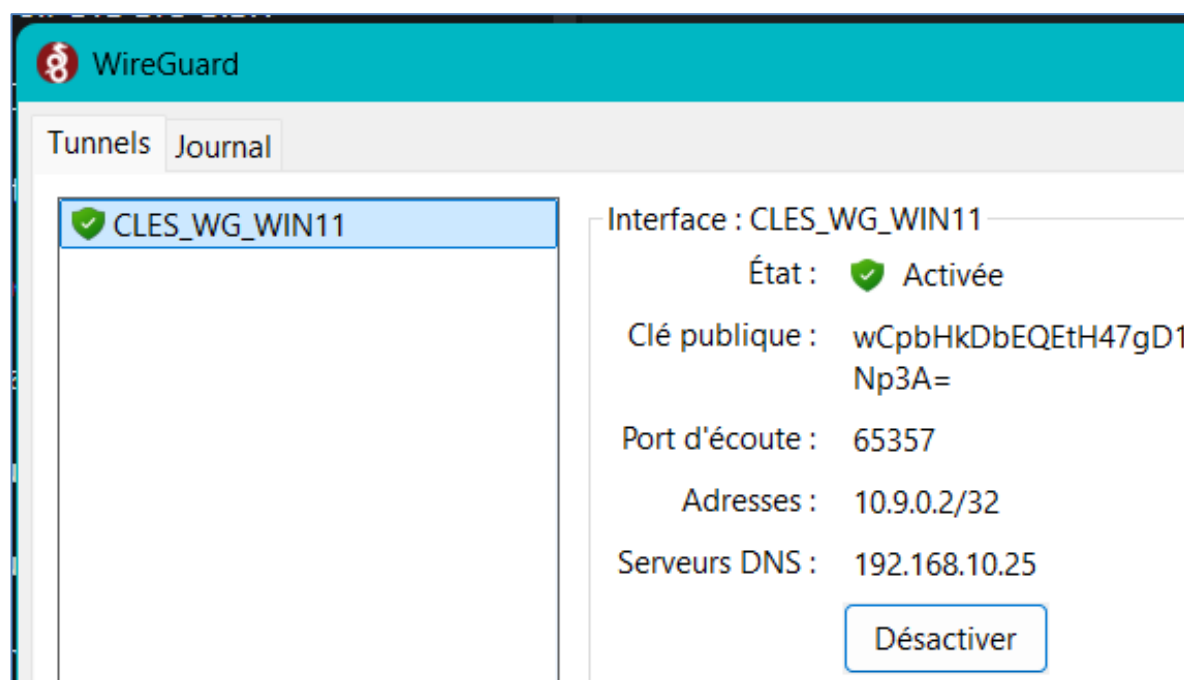
Enregistrer Annuler

Vos paramètres WireGuard s'affichent désormais :

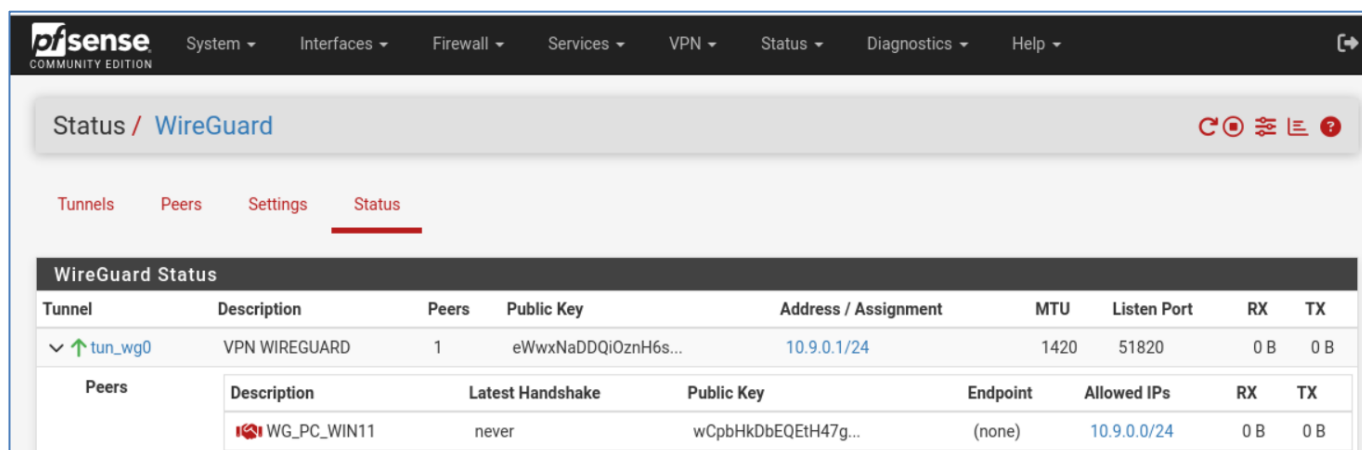


7 – ACTIVATION ET TESTS

- Depuis la machine cliente Windows, ouvrez l'outil WireGuard et cliquez le bouton « Activer » ; si tout est correct, vous obtenez ceci (le statut de l'état doit être en vert avec la mention « Activée ») :



- Depuis l'interface de gestion de pfSense, cliquez sur « Status » - « WireGuard » ; vous devez obtenir ceci (une petite flèche verte s'affiche au niveau du tunnel) :



WireGuard Status

Tunnel	Description	Peers	Public Key	Address / Assignment	MTU	Listen Port	RX	TX
✓ ↑ tun_wg0	VPN WIREGUARD	1	eWwxNaDDQiOznH6s...	10.9.0.1/24	1420	51820	0 B	0 B

Peers		Description	Latest Handshake	Public Key	Endpoint	Allowed IPs	RX	TX
❌	WG_PC_WIN11		never	wCpbHkDbEQEtH47g...	(none)	10.9.0.0/24	0 B	0 B

A ce stade votre environnement est prêt. Il ne vous reste plus qu'à définir les règles nécessaires dans votre pare-feu afin d'autoriser les connexions entrantes et sortantes.

A vous de jouer !